WHAT IS CLAIMED IS:

1. A computer system operating in a network environment for preventing security breaches, comprising:

an interface layer that receives at least one connection request from another computer; and

a security layer that examines the connection request, gathers a list of router addresses and compares the router addresses to a set of known firewall router address.

2. The computer system of claim 1, wherein the security layer generates an alert to a user of the computer if one of the gathered addresses match one of the known firewall router addresses.

3. The computer system of claim 2, wherein the security layer provides the user of the computer the option to grant or deny the connection request.

4. The computer system of claim 1, wherein the security layer denies the connection request if one of the gathered addresses match one of the known firewall router addresses.

5. The computer system of claim 1, wherein the security layer uses a traceroute to gather the list of router addresses.

6. The computer system of claim 5, wherein the traceroute gathers Internet Protocol (IP) addresses of all routers between the computer system and a machine originating the connection request.

7. The computer system of claim 1, further comprising a socket layer residing above the security layer and coupling connection requests to data stored on the computer.

8. The computer system of claim 6, wherein the security layer resides between the socket layer and the interface layer.

9. The computer system of claim 1, wherein the security layer monitors Transmission Control Protocol (TCP) data packets for synchronization (SYN) requests.

10. A computer implemented method operating in a network environment for preventing security breaches, comprising:

receiving at least one connection request from another computer;

gathering a list of router addresses associated with the connection request; and

comparing the router addresses to a set of known firewall router address.

11. The method of claim 10, further comprising alerting a user of the computer if one of the gathered addresses match one of the known firewall router addresses.

12. The method of claim 10, further comprising providing a user of the computer the option to grant or deny the connection request.

13. The method of claim 10, further comprising denying the connection request if one of the gathered addresses match one of the known firewall router addresses.

14. The method of claim 10, further comprising using a traceroute to gather the list of router addresses.

15. The method of claim 14, wherein the traceroute gathers Internet Protocol (IP) addresses of all routers between the computer system and the machine originating the connection request.

16. A computer-readable medium having computer-executable instructions operating on a computer system for validating connection requests on a networked computer, comprising:

an interface module operating on the computer that examines the

connection request and collects Internet Protocol (IP) addresses of all routers between the computer and a machine originating the connection request; and

a security module that compares the collected addresses to a set of known firewall router address and prevents the connection request if the any of the collected addresses match the set of known firewall addresses.

17. The computer-readable medium of claim 16, wherein an alert is provided to a user of the computer if one of the gathered addresses match one of the known firewall router addresses.

18. The computer-readable medium of claim 16, wherein the security module provides a user of the computer the option to grant or deny the connection request.

19. The computer-readable medium of claim 16, wherein the interface module uses a traceroute to collect the router addresses.

20. The computer-readable medium of claim 16, wherein the security module monitors Transmission Control Protocol (TCP) data packets for synchronization (SYN) requests.